Dennis Stewart, CA Bar No. 99152
GUSTAFSON GLUEK PLLC
600 W. Broadway, Suite 3300
San Diego, CA 92101
Telephone: (619) 595-3299

Attorney for Plaintiff and Proposed Class
(Additional Counsel on Signature Page)

UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF CALIFORNIA

PETER HAHN, on behalf of himself and all others similarly situated,

Plaintiff,

v.

VISON SERVICES PLAN a/k/a VSP GLOBAL; VSP VENTURES, LLC; VSP VENTURES MANAGEMENT SERVICES, LLC; and VSP VENTURES OPTOMETRIC SOLUTIONS, LLC,

Defendants.

Case No.

CLASS ACTION COMPLAINT FOR:

1. **VIOLATION OF THE ELECTRONIC PRIVACY ACT, 18 U.S.C. § 2510, *et seq.***
2. **VIOLATIONS OF CAL. PENAL CODE § 631, *et seq*.;**
3. **VIOLATIONS OF CAL. PENAL CODE § 638.51(a);**
4. **VIOLATIONS OF CAL. CIV. CODE § 56, *et seq*.;**
5. **VIOLATIONS OF CAL. BUS. & PROF. CODE § 17200, *et seq.*;**
6. **CONVERSION**

JURY TRIAL DEMANDED

Plaintiff Peter Hahn ("Plaintiff") bring this action on behalf of themselves, and all others similarly situated against Defendants Vision Service Plan (a/k/a VSP Global); VSP Ventures, LLC; VSP Ventures Management Services, LLC; and VSP Ventures Optometric Solutions, LLC (collectively "VSP" or "Defendant"). VSP owns and controls VSP.com, chooseVSP.com, visoncare.VSP.com, VSPdirect.com, and related webpages (the "Website"), and it also owns and controls a mobile app (the "App") (collectively, the "Web Properties").

NATURE OF THE ACTION

1. Plaintiff brings this class action against VSP for its failure to properly secure and safeguard its patients' sensitive health information, including details about their medical conditions, prescriptions, doctors' appointments, and other information submitted on VSP's Web Properties.

2. Defendant offers vision care benefit plans through its Website and App. These Website Properties also allow patients and plan members to connect with doctors and vision care services. Through the Website and App, patients can search for providers in their local area and connect with providers to book an appointment. Patients can also search for eye doctors and optometrists, learn about various eye conditions, pay for medical eye services, explore eye care insurance options, shop for eyewear and accessories, and more.[1]

3. VSP's patients communicate their private information via the site, including details about their medical conditions and treatments related to their eyes.

4. VSP owns and controls the Web Properties, which it encouraged Plaintiff and other patients to use for: (1) coordinating their care; (2) obtaining information about their upcoming treatments, therapies, and procedures; (3) identifying in-network providers that meet their unique search criteria; (4) using online calculators to determine their "Cost and Coverage;" (5) enrolling in vision insurance; (6) comparing insurance plans; (7) completing referral requests, forms, quizzes, and other types of dynamic forms; (8) making online payments; and (9) registering for their vision insurance account.

[1] *See* VSP VISION CARE, VSP.com (last accessed May 1, 2024).

5. In doing so, and by designing its Web Properties in the manner described throughout this complaint, VSP knew or should have known that its patients would use the Web Properties to communicate Private Information in conjunction with obtaining and receiving medical services and insurance from VSP.

6. By installing and using Tracking Technologies on its Web Properties, VSP effectively planted a bug on Plaintiff's and Class Members' web browsers and devices, which caused their communications to be intercepted, accessed, viewed, and captured by third parties in real time, as they were communicated by patients, based on VSP's chosen parameters.

7. For example, VSP used the Meta Pixel, which "tracks the people and [the] type of actions they take"[1] in real time as they interact with a website, including the exact text and phrases that patients typed into various portions of the Web Properties. Operating as designed and as implemented by VSP, the Meta Pixel and other Tracking Tools caused Plaintiff's and Class Members' Private Information to be unlawfully intercepted and surreptitiously disclosed to third parties.

8. The Office for Civil Rights at HHS has issued a Bulletin to highlight the obligations of entities and business associates covered by the Health Insurance Portability and Accountability Act ("HIPAA") ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technologies ("tracking technologies"), such as the Tracking Technologies.[2] The Bulletin expressly provides (in bold type) that "**[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.**" In other words, HHS has expressly stated that VSP's implementation of Tracking Technologies violates HIPAA Rules.

9. The information VSP divulged to unauthorized third parties—Meta, Google, and LinkedIn—allowed those entities to learn that specific individuals were patients seeking and receiving treatment at VSP's vision clinics and other medical centers. In and of itself, this reveals the fact that an individual is being treated for vision problems and has received or will receive

vision services. In turn, this information was used and/or sold to additional unauthorized parties for use in marketing and geotargeting.

10. Patients simply do not anticipate that their trusted healthcare and insurance provider will send their Private Information to social media and marketing companies for future exploitation and targeted marketing.

11. Neither Plaintiff nor any other Class Member signed a written authorization permitting VSP to send their Private Information to Meta, Google, or LinkedIn.

12. Similarly, VSP does not have a HIPAA-compliant Business Associate Agreement in place with Meta, Google, or LinkedIn.

13. As a healthcare provider, VSP is required by law to provide every patient with a Notice of Privacy Practices. In its Notice of Privacy Practices, VSP states that it is "required by law to maintain the privacy and security of [patient's] protected health information."[2]

14. Despite VSP's promise to maintain the privacy and security of its patients' sensitive health information, VSP nevertheless intentionally chose to embed the Meta and Google trackers on its Web Properties, sharing Plaintiff's and Class Members' sensitive health information with Meta and Google without their consent when they communicated with VSP's Web Properties.

15. The disclosure of Plaintiff's and Class Members' sensitive health information enabled Meta and Google to gain intimate insight into the types of medical care and medical treatments patients sought from VSP.

16. As described in this Complaint, VSP did not reasonably protect, secure, or store Plaintiff's and Class Members' sensitive health information, but rather intentionally and knowingly granted Meta and Google access to their confidential information.

17. VSP's actions constitute a reckless disregard for the privacy of patients' sensitive health information and its duties as a healthcare provider, an extreme invasion of Plaintiff's and Class Members' right to privacy, and a violation of state statutory and common law.

[2] *Notice of Privacy Practice*, VSP, https://www.vsp.com/legal/nopp (last visited May 1, 2024).

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 because this action arises under 18 U.S.C. § 2510, et seq. (the Electronic Communications Privacy Act). This Court also has subject matter jurisdiction under 28 U.S.C. § 1332(d) (the Class Action Fairness Act) because the proposed class exceeds 100 persons, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and a member of the Class is a citizen of a different state from VSP's home state.

19. This Court has supplemental jurisdiction over the state law claims under 28 U.S.C. § 1367 because the state law claims form part of the same case or controversy under Article III of the United States Constitution.

20. This Court has personal jurisdiction over Defendant because its corporate headquarters is located in this District.

21. Venue is proper in this District because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

PARTIES

A. Plaintiff Peter Hahn

22. Plaintiff Peter Hahn is a resident of Itasca, IL. Mr. Hahn visited and used Defendant's Website in July 2024, while he was a VSP member, to look at his vision insurance, check his benefits, and find a doctor.

23. Pursuant to the systematic process described herein, Defendant assisted Meta and Google with intercepting Mr. Hahn's communications, including those that contained personally identifiable information, protected health information, and related confidential information. Defendant assisted these interceptions without Mr. Hahn's knowledge, consent, or express written authorization.

24. By failing to receive the requisite consent, Defendant breached its duties of confidentiality and unlawfully disclosed Plaintiff Hahn's personally identifiable information and protected health information.

B. Defendant VSP

25. Defendant Vision Service Plan a/k/a VSP Global is incorporated in California and has a principal place of business at 3333 Quality Drive, Rancho Cordova, California 95670.[3]

26. VSP Ventures, LLC is a Delaware limited liability company owned and operated by Vision Service Plan. On information and belief, VSP Ventures, LLC is headquartered at 3333 Quality Drive, Rancho Cordova, California 95670, which is located in this District.

27. VSP Ventures Management Services, LLC is a Delaware limited liability company owned and operated by Vision Service Plan. On information and belief, VSP Ventures Management Services, LLC is headquartered at 3333 Quality Drive, Rancho Cordova, California 95670, which is located in this District.

28. VSP Ventures Optometric Solutions, LLC is a Delaware limited liability company owned and operated by Vision Service Plan. On information and belief, VSP Ventures Optometric Solutions, LLC is headquartered at 3333 Quality Drive, Rancho Cordova, California 95670, which is located in this District.

FACTUAL ALLEGATIONS

A. Background

1. The Electronic Communications Privacy Act

29. The Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2510, *et seq*., prohibits the intentional interception of the contents of any electronic communication or inducing another to intercept any electronic communication. 18 U.S.C. § 2511.

30. As relevant here, a defendant violates 18 U.S.C. § 2511(1)(a) when it: "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."

31. The ECPA applies to software and not just traditional wiretapping technology. *See Yockey v. Salesforce, Inc.*, 2024 WL 3875785, at *8 (N.D. Cal. Aug. 16, 2024) (affirming that the ECPA applies to software); *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1087 (N.D. Cal. 2015)

[3] *See Contact VSP Vision*, VSP, https://vspvision.com/utility/contact.html (last visited May 1, 2024).

("Carrier IQ Software is an '[e]lectronic, mechanical, or other device' which 'can be used to intercept a wire, oral, or electronic communication" pursuant to the federal Wiretap Act); *United States v. Hutchins*, 361 F. Supp. 3d 779, 795 (E.D. Wis. 2019) ("The majority of courts to consider this issue have entertained the notion that software may be considered a device for the purposes of the Wiretap Act.") (citations omitted).

32. The ECPA also provides a private right of action to obtain declaratory relief, reasonable fees, and damages for the greater of: (a) actual damages and any profits made by the violator as a result of the violation or (b) statutory damages of $100 a day for each violation or $10,000. 18 U.S.C. § 2520.

2. The California Invasion of Privacy Act

33. The California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 630, *et seq*., prohibits aiding or permitting another person to willfully—and without the consent of all parties to a communication—read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from or received at any place within California.

34. As relevant here, a defendant violates § 631(a) of CIPA when the defendant "by means of any machine, instrument, contrivance, or in any other manner" does any of the following:

> Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system; or
>
> Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within California; or
>
> Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained; or
>
> Aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above.

Cal. Penal Code § 631.

35. Section 631(a) applies not only to phone lines, but also to "new technologies" such as computers, the internet, and email. *See Matera v. Google Inc.*, No. 15-CV-04062-LHK, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc.*, No. C 06-05289 WHA, 2006 WL 3798134, at *5–6 (N.D. Cal. Dec. 22, 2006) (CIPA governs "electronic communications"); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of consumers' internet browsing history).

36. Moreover, § 638.51(a) of CIPA proscribes any "person" from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

37. A "pen register" is a "device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

38. By contrast, a "trap and trace device" is a "device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." *Id.*

39. A "pen register" is a "device or process" that records outgoing information, whereas a "trap and trace device" is a "device or process" that recording incoming information.

40. Although CIPA was enacted before the creation of the Tracking Technologies employed by Defendant, "the California Supreme Court regularly reads statutes to apply to new technologies where such a reading would not conflict with the statutory scheme." *In re Google Inc.*, No. 13-MD-02430-LHK, 2013 WL 5423918, at *21 (N.D. Cal. Sep. 26, 2013); *see also, e.g., Shah v. Fandom, Inc*, 754 F. Supp. 3d 924, 930 (N.D. Cal. 2024) (finding trackers similar to those at issue here were "pen registers" and noting "California courts do not read California statutes as

limiting themselves to the traditional technologies or models in place at the time the statutes were enacted").

41. Under CIPA, Plaintiff and Class Members may seek injunctive relief and statutory damages of $5,000 per violation. Cal. Penal Code § 637.2.

3. The California Confidentiality of Medical Information Act

42. Pursuant to the California Confidentiality of Medical Information Act ("CMIA"), "[a] provider of health care . . . shall not disclose medical information regarding a patient of the provider of health care . . . without first obtaining an authorization, except as provided in subdivision (b) or (c)." § 56.10(a). Under the CMIA, an authorization for the release of medical information is valid only if the release:

> (a) Is handwritten by the person who signs it or is in a typeface no smaller than 14-point type.
>
> (b) Is clearly separate from any other language present on the same page and is executed by a signature which serves no other purpose than to execute the authorization.
>
> (c) Is signed and dated . . .
>
> (d) States the specific uses and limitations on the types of medical information to be disclosed.
>
> (e) States the name or functions of the provider of health care, health care service plan, pharmaceutical company, or contractor that may disclose the medical information.
>
> (f) States the name or functions of the persons or entities authorized to receive the medical information.
> (g) States the specific uses and limitations on the use of the medical information by the persons or entities authorized to receive the medical information.
>
> (h) States a specific date after which the provider of health care, health care service plan, pharmaceutical company, or contractor is no longer authorized to disclose the medical information.
>
> (i) Advises the person signing the authorization of the right to receive a copy of the authorization.

Cal. Civ. Code § 56.11.

43. Moreover, a health care provider that maintains information for purposes covered by the CMIA is liable for negligent disclosures that arise as the result of an affirmative act—such

as implementing a system that records and discloses online patients' personally identifiable information and protected health information. Cal. Civ. Code § 56.36(c).[4] Similarly, if a negligent release occurs and medical information concerning a patient is improperly viewed or otherwise accessed, the individual need not suffer actual damages. *Id.* § 56.36(b).

44. The CMIA allows any individual to:

> bring an action against any person or entity who has negligently released confidential information or records concerning them in violation of this part, for either or both of the following: [¶] (1) . . . nominal damages of one thousand dollars ($1,000). To recover under this paragraph, it shall not be necessary that the Plaintiffs suffered or was threatened with actual damages. [¶] (2) The amount of actual damages, if any, sustained by the patient.

Sutter Health v. Superior Ct., 174 Cal. Rptr. 3d 653, 656 (Cal. Ct. App. 2014) (quoting Cal. Civ. Code § 56.36(b)) (internal quotation marks omitted).

4. Meta's Business Tools and the Pixel

45. Meta operates the world's largest social media company and generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[7]

46. In conjunction with its advertising business, Meta encourages and promotes entities and website owners, such as Defendant, to utilizes its "Business Tools" to gather, identify, target, and market products and services to individuals.

47. Meta's Business Tools, including the Pixel and Conversions API, are bits of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of mobile app and website visitors' activity.

48. One such Business Tool is the Pixel, which "tracks the people and type of actions they take."[8] When a user accesses a webpage hosting the Pixel, their communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Meta's servers.

[4] *See also* Cal. Civ. Code § 56.101(a) ("Every provider of health care ... who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein. Any provider of health care ... who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36.").

49. Notably, these transmissions to Meta do not occur unless the webpage or mobile app contains the Meta Pixel or another Meta Business Tool. Stated differently, Plaintiff's and Class Members' Private Information would not have been disclosed to Meta but for VSP's decision to install and use Meta Business Tools on its Web Properties.

50. These secret transmissions to Meta are initiated by VSP's source code concurrently with Plaintiff's and Class Members' communications to their intended recipient, VSP.

5. Google Analytics and tracking Technologies

51. Third parties, like Google, offer Tracking Tools as software that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of user communications and activity on those platforms. The Tracking Tools are used to gather, identify, target, and market products and services to individuals.

52. In general, Tracking Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, that webpage's URL and metadata, button clicks, etc. Advertisers, such as Defendant, can track other user actions and communications and can create their own tracking parameters by customizing the software on their website.

53. When a user accesses a webpage that is hosting Tracking Tools, the user's communications with the host webpage are instantaneously and surreptitiously duplicated and sent to the third party. For example, the Google Analytics tool on Defendant's Website causes the user's web browser to instantaneously duplicate the contents of the communication with the Website and send the duplicate from the user's browser directly to Google Analytics server.

54. Google Analytics tracks what a user communicates to Defendant's website.[5]

[5] *Comparing Google Analytics vs Facebook Pixel*, Boltic, https://www.boltic.io/blog/google-analytics-vs-facebook-pixel#:~:text=Google%20Analytics%20is%20a%20comprehensive,time%20on%20site%2C%20and%20conversions.&text=On%20the%20other%20hand%2C%20Facebook,user%20actions%20on%20your%20website. (last visited Jan. 26, 2024)

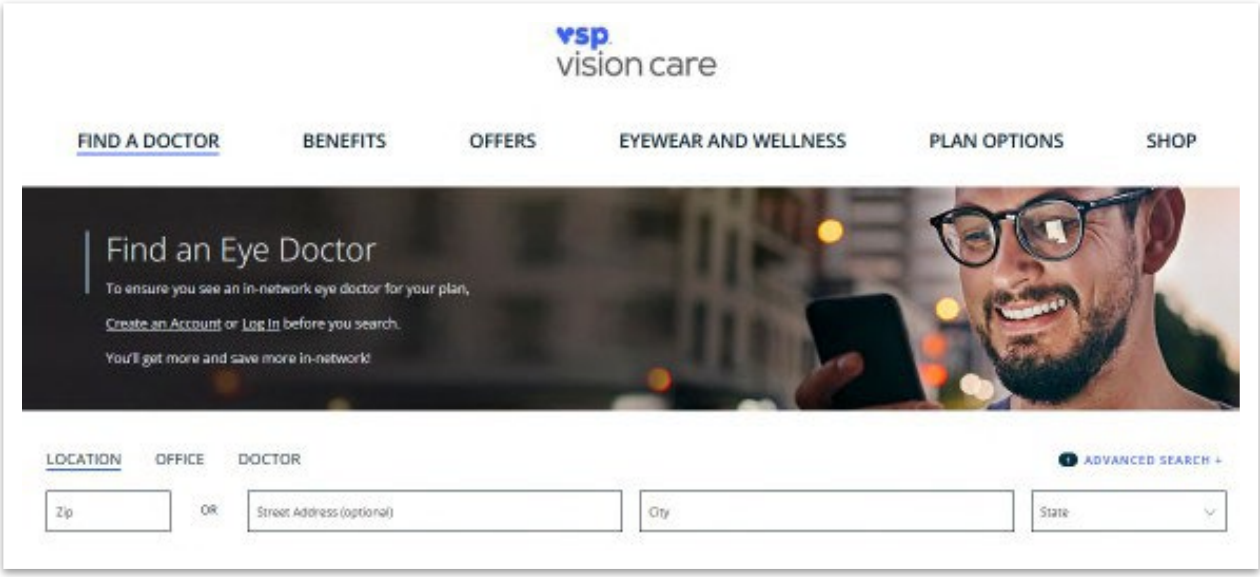
55. Notably, transmissions only occur on webpages that contain Tracking Tools.[6] Thus, Plaintiff's and Class Member's Private Information would not have been disclosed to Google via this technology but for Defendant's decisions to install the Tracking Tools on its Website.

B. VSP Disclosed Plaintiff's and Class Members' Protected Health Information and Assisted with Intercepting Communications.

56. Upon entering Defendant's Website, users can simply browse the Website or log into their account. When users log into their accounts, their VSP membership status and login activities are shared with both Google and Meta (see images below).

[6] Defendant's Google Analytics tool stores a client ID in a first-party cookie named _ga (also identified as a cid) to distinguish unique users and their sessions on your website. Analytics doesn't store the client ID when analytics storage is disabled through Consent Mode." https://support.google.com/analytics/answer/11593727?hl=en#:~:text=Google%20Analytics%20stores%20a%20client,is%20disabled%20through%20Consent%20Mode. (last visited Jan. 26, 2024).

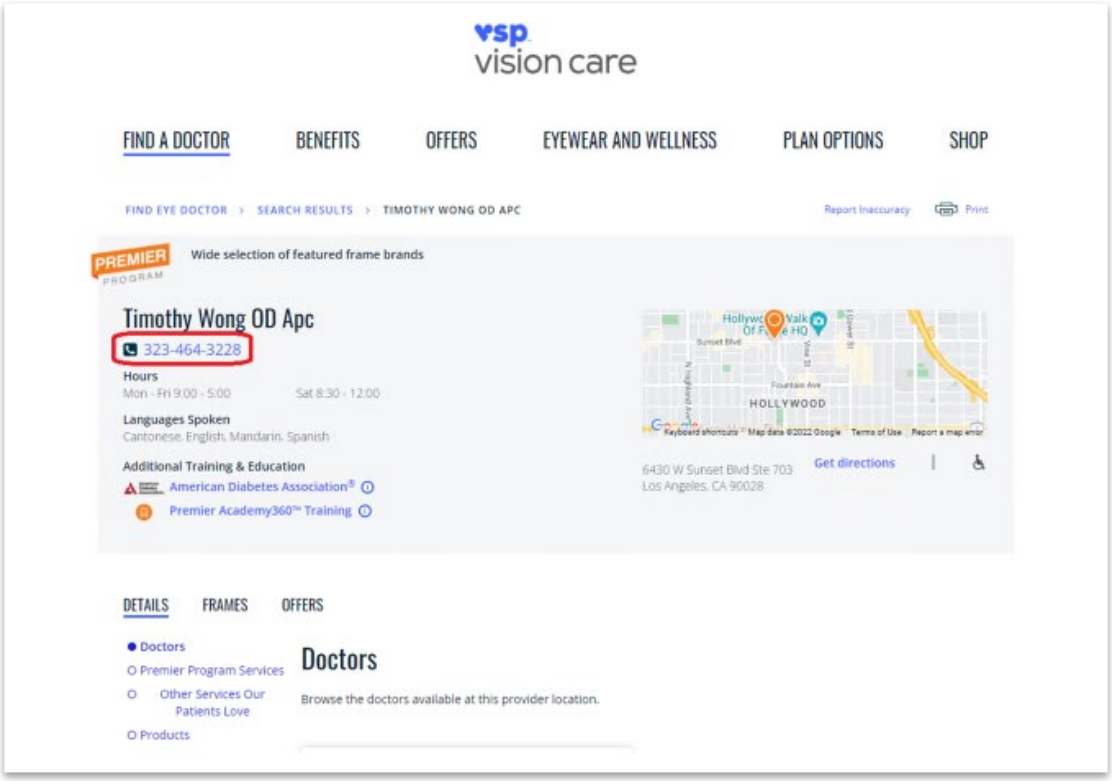
57. Whether logged in or just browsing the Website, users can search for a doctor by navigating to the "Find a Doctor" page, where they are able to search for a doctor by name, office, and location:

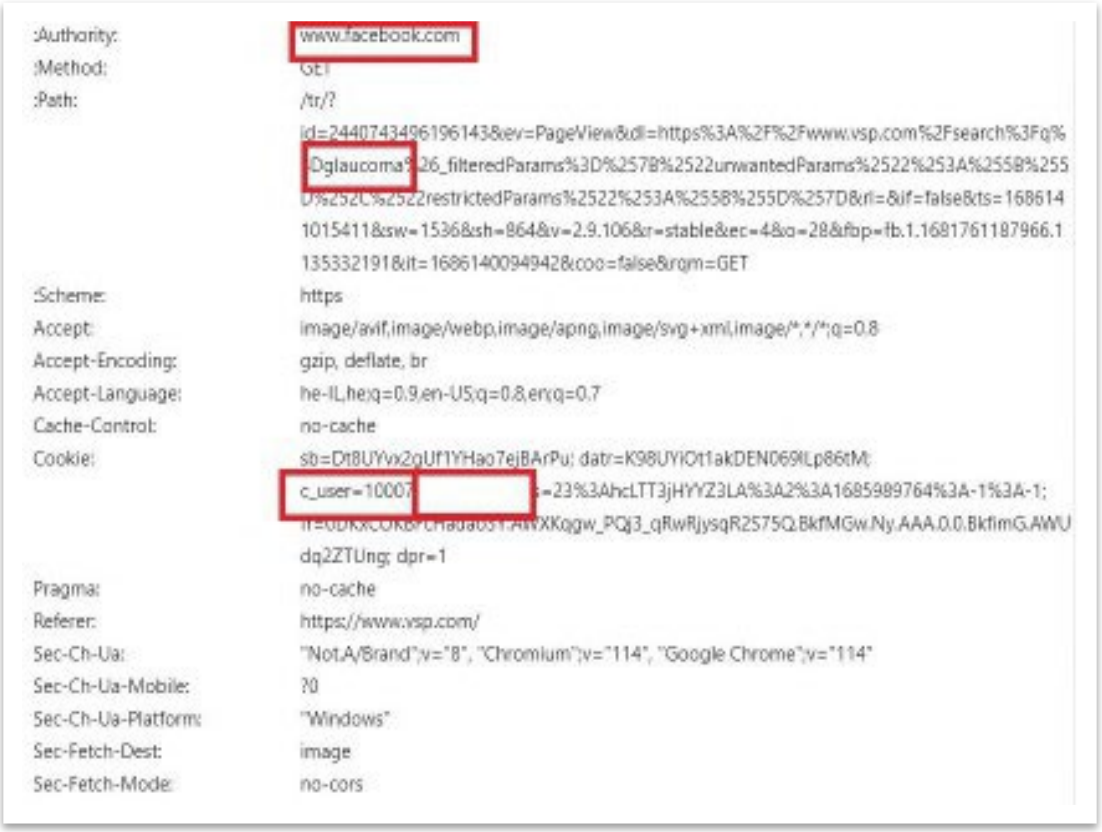


58. Additionally, they can use the advanced search option to filter by type of doctor, service, location, gender, language and more.

59. After searching for a doctor, their submitted information is automatically sent to Meta and Google through the Meta Pixel and Google Analytics, respectively. As shown in the example images below, VSP's site transmits to Meta and Google the following information associated with user's PII and protected health information: the user searched for a male optometrist who has a practice located within 50 miles of zip code 90004, provides eye exams, and speaks English. All information collected through the Meta Pixel and Google Analytics in this way is simultaneously and contemporaneously sent to Meta's and Google's servers at the time of collection.

60. After the user selects a doctor from the search results page, VSP transmits the name of the doctor to Meta and Google. As shown in the example images below, VSP transmits to Meta and Google that the user clicked on the profile page of a particular doctor—for example, Dr. Timothy Wong OD APC—along with whether the patient clicked on the doctor's phone number to contact them.





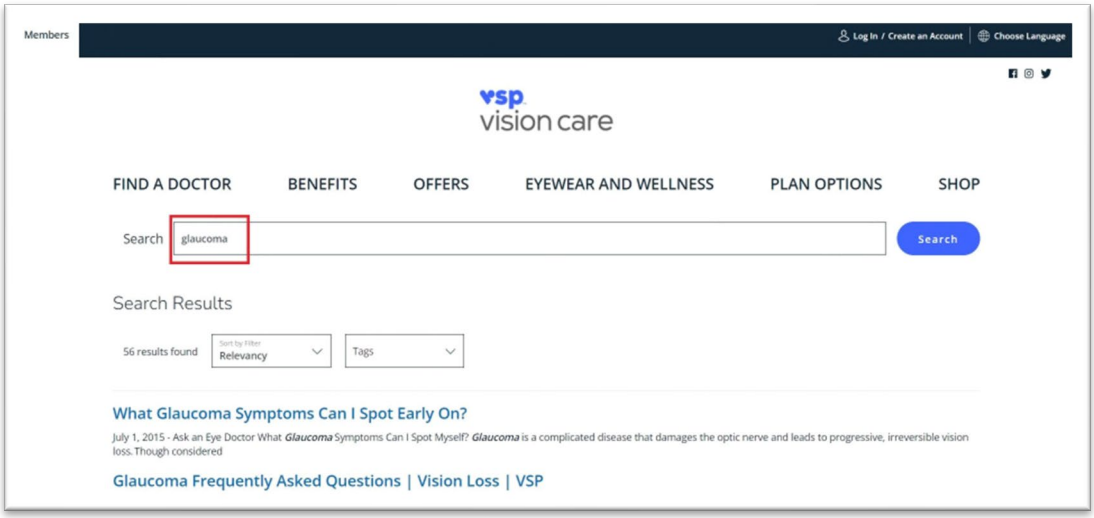
:Authority:	www.facebook.com
:Method:	GET
:Path:	/tr/? id=2440743496196143&ev=PageView&dl=https%3A%2F%2Fwww.vsp.com%2Fsearch%3Fq% 3Dglaucoma%26_filteredParams%3D%2578%2522unwantedParams%2522%253A%2558%255 D%252C%2522restrictedParams%2522%253A%2558%255D%257D&rl=&if=false&ts=168614 1015411&sw=1536&sh=864&v=2.9.106&r=stable&ec=4&o=28&fbp=fb.1.1681761187966.1 1353321918&it=1686140094942&coo=false&rqm=GET
:Scheme:	https
Accept:	image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Encoding:	gzip, deflate, br
Accept-Language:	he-IL,he;q=0.9,en-US;q=0.8,en;q=0.7
Cache-Control:	no-cache

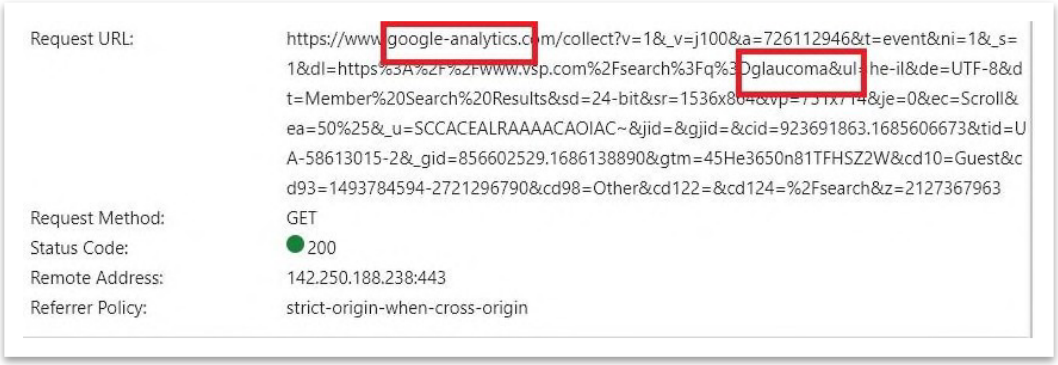
Cookie:	sb=Dt8UYvx2gUf1YHao7ejBArPu; datr=K98UYiOt1akDEN069fLp86tM;
	c_user=10007[redacted]=23%3AhcLTT3jHYYZ3LA%3A2%3A1685989764%3A-1%3A-1;
	[redacted]dq2ZTUng; dpr=1

Pragma:	no-cache
Referer:	https://www.vsp.com/
Sec-Ch-Ua:	"Not.A/Brand";v="8", "Chromium";v="114", "Google Chrome";v="114"
Sec-Ch-Ua-Mobile:	?0
Sec-Ch-Ua-Platform:	"Windows"
Sec-Fetch-Dest:	image
Sec-Fetch-Mode:	no-cors

:authority: www.google-analytics.com
:method: GET
:path: /collect?v=1&_v=j98&a=949483212&t=event&ni=0&_s=1&dl=https%3A%2F%2Fwww.vsp.com%2Feye-doctor%2Fpractice%2FCA%2Flos-angeles%2F6430-w-sunset-blvd-ste-703%2Ftimothy-wong-od-apc%2F93648&ul=en-us&de=UTF-8&dt=Timothy%20Wong%20OD%20Apc%20%7C%20VSP%20Eye%20Doctor%20Near%20Me&sd=24-bit&sr=1920x1080&vp=950x929&je=0&ec=Outbound%20Link%20Click&ea=www.vsp.com&el=%20-%2323-464-3228&_u=SDCACEALRAAAACAOK~&jid=&gjid=&cid=1519611142.1663586741&tid=UA-58613015-55&_gid=1632815375.1669022948&gtm=2wgb90TFH5Z2W&cd10=Guest&cd93=539563685-4268097347&cd122=https%3A%2F%2Fwww.vsp.com%2Feye-doctor%2Fstate-search&cd124=%2Feye-doctor%2Fpractice%2FCA%2Flos-angeles%2F6430-w-sunset-blvd-ste-703%2Ftimothy-wong-od-apc%2F93648&z=172156432
:scheme: https
accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
accept-encoding: gzip, deflate, br
accept-language: en-US,en;q=0.9,he-IL;q=0.8,he;q=0.7
referer: https://www.vsp.com/

61. Further, any information submitted by the user through the search bar (e.g., doctor, specialty, type of treatment, etc.) on the site's homepage is shared with Meta and Google, as demonstrated in the images below.





62. In short, nearly all of the information that users submit to VSP's Web Properties will be surreptitiously and simultaneously transmitted to Facebook and Google without the user's consent.

63. VSP knowingly and intentionally installed Meta Pixel and Google Analytics to collect user data and in doing so VSP failed to take reasonable steps to secure and protect its users' information from unnecessary, non-consensual disclosure. Instead, VSP knowingly and intentionally granted third parties the ability to surreptitiously record and collect user information. The Meta Pixel and Google's Analytics platforms cannot be installed accidentally. VSP purposely installed both platforms on its Web Properties with the intent of collecting data about patients.

C. VSP Violated both Industry Standards and Federal Warnings Regarding Tracking Codes on Healthcare Websites

64. Defendant's tracking of user behavior falls well outside of users' reasonable expectations of privacy regarding their health data. For example, the American Medical Association's (the "AMA") Code of Ethics lists "safeguard[ing] patient confidences and privacy" as one of its core principles.[7]

65. Further, AMA ethics opinion 3.2.4 regarding access to medical records by data collection companies reads in part:

> Information gathered and recorded in association with the care of a patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information to third parties for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship.[8]

66. In addition, the federal government has issued guidance warning that tracking code like the Meta Pixel and Google Analytics may violate federal privacy law when installed on healthcare websites like VSP's. The statement—titled Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates (the "Bulletin")—was issued by the Department of Health and Human Services' Office for Civil Rights ("OCR") in December 2022 and further clarified in March 2024.[9]

67. Healthcare organizations regulated under HIPAA may use third-party tracking tools, such as the Meta Pixel and Google Analytics, in a limited way, to perform analysis as part of the entity's health care operations, such as gathering innocuous data which does not include patient information. They are however, not permitted to use these tools in a way that may cause an

---

[7] *Code of Medical Ethics*, American Medical Association, https://code-medical-ethics.ama- assn.org/principles.

[8] *Opinion 3.2.4 Access to Medical Records by Data Collection Companies*, American Medical Association, https://code-medical-ethics.ama-assn.org/ethics-opinions/access-medical-records- data-collection-companies.

[9] *Use Of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, HHS, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last accessed May 1, 2024).

unauthorized exposure of patients' Protected Health Information ("PHI") to external vendors. The Bulletin explains:

> **Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.** For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.[10]

68. Further, the Bulletin discusses how businesses associated with covered entities may violate HIPAA with similar disclosures of PHI:

> Furthermore, tracking technology vendors are business associates if they create, receive, maintain, or transmit PHI on behalf of a regulated entity for a covered function (e.g., health care operations) or provide certain services to or for a covered entity (or another business associate) that involve the disclosure of PHI. In these circumstances, regulated entities must ensure that the disclosures made to such vendors are permitted by the Privacy Rule and enter into a business associate agreement (BAA) with these tracking technology vendors to ensure that PHI is protected in accordance with the HIPAA Rules. For example, if an individual makes an appointment through the website of a covered health clinic for health services and that website uses third party tracking technologies, then the website might automatically transmit information regarding the appointment and the individual's IP address to a tracking technology vendor. In this case, the tracking technology vendor is a business associate, and a BAA is required.[11]

69. The Bulletin discusses the types of harm that disclosures of PHI may cause to a patient:

> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.[12]

[10] *Id.* (emphasis in original).

[11] *Id.*

[12] *Id.*

70. Plaintiffs and Class Members face exactly the risks highlighted in the Bulletin. VSP disclosed to Meta and Google that Plaintiffs and Class Members sought out or took steps to book ophthalmologic care on VSP's website, which in turn also disclosed the health conditions for which a health care provider was sought; the frequency with which the Plaintiff or Class Member takes steps relating to obtaining eye health care; and where they seek medical treatment. Per the Bulletin, this information is "incredibly sensitive."

71. The Bulletin goes on to discuss the exact nature of the disclosures required and how standard disclosures like privacy policies, notices, cookie policies, or even de-identification would not meet the bar required under HIPAA. The Bulletin says:

> Regulated entities may identify the use of tracking technologies in their website or mobile app's privacy policy, notice, or terms and conditions of use. However, the Privacy Rule does not permit disclosures of PHI to a tracking technology vendor based solely on a regulated entity informing individuals in its privacy policy, notice, or terms and conditions of use that it plans to make such disclosures. … If there is not an applicable Privacy Rule permission or if the vendor is not a business associate of the regulated entity, then the individuals' HIPAA-compliant authorizations are required before the PHI is disclosed to the vendor. Website banners that ask users to accept or reject a website's use of tracking technologies, such as cookies, do not constitute a valid HIPAA authorization. … Further, it is insufficient for a tracking technology vendor to agree to remove PHI from the information it receives or de-identify the PHI before the vendor saves the information. Any disclosure of PHI to the vendor without individuals' authorizations requires the vendor to have a signed BAA in place **and** requires that there is an applicable Privacy Rule permission for disclosure.[13]

72. To be clear, VSP's conduct violates the rules outlined by the AMA and the OCR's Bulletin regarding the appropriate use of tracking technologies on websites.

[13] *Id.* (emphasis in original).

CLASS ALLEGATIONS

73. **Class Definition**: Plaintiff bring this action on behalf of himself and other similarly situated individuals (the "Class"), defined as United States citizens who, during the Class Period, had their personally identifiable information or protected health information disclosed to Meta or Google as a result of using www.VSP.com.

74. Plaintiff reserves the right to modify the class definition or add subclasses as necessary prior to filing a motion for class certification.

75. The "Class Period" is the time period beginning on the date established by the Court's determination of any applicable statute of limitations, after consideration of any tolling, concealment, and accrual issues, and ending on August 1, 2024.

76. Excluded from the Federal Law Class is Defendant; any affiliate, parent, or subsidiary of Defendant; any entity in which Defendant has a controlling interest; any officer, director, or employee of Defendant; any successor or assign of Defendant; anyone employed by counsel in this action; any judge to whom this case is assigned, his/her spouse and immediate family members; and members of the judge's staff.

77. **Numerosity/Ascertainability**: Members of the Class are so numerous that joinder of all members would be unfeasible and not practicable. The exact number of Class Members is unknown to Plaintiffs at this time; however, it is estimated that there are hundreds of thousands of individuals in the Class. The identity of such membership is readily ascertainable from Defendant's records and non-party Meta's and Google's records.

78. **Typicality**: Plaintiff's claims are typical of the claims of the Class because Plaintiff used VSP's Web Properties and had his personally identifiable information and protected health information disclosed to Meta and Google without his express written authorization or knowledge. Plaintiff's claims are based on the same legal theories as the claims of Class members.

79. **Adequacy**: Plaintiff is fully prepared to take all necessary steps to represent fairly and adequately the interests of the Class Members. Plaintiff's interests are coincident with, and not antagonistic to, those of the members of the Class. Plaintiff is represented by attorneys with experience in the prosecution of class action litigation, generally, and in the emerging field of

digital privacy litigation, specifically. Plaintiff's attorneys are committed to vigorously prosecuting this action on behalf of the members of the Class.

80. **Common Questions of Law and Fact Predominate/Well Defined Community of Interest**: Questions of law and fact common to the members of the Class predominate over questions that may affect only individual members of the Class because Defendant has acted on grounds generally applicable to the Class. Such generally applicable conduct is inherent in Defendant's wrongful conduct. Questions of law and fact common to the Classes include:

a) Whether Defendant intentionally tapped the lines of internet communication between patients and their health providers;

b) Whether VSP's website surreptitiously records personally identifiable information, protected health information, and related communications and subsequently, or simultaneously, discloses that information to Meta and Google;

c) Whether Meta and Google are third-party eavesdroppers;

d) Whether Defendant's disclosures of personally identifiable information, protected health information, and related communications constituted an affirmative act of communication;

e) Whether Defendant's disclosure of Plaintiff's and Class Members' personally identifiable information and protected health information to unauthorized third parties—Meta and Google—resulted in a breach of confidentiality;

f) Whether Defendant violated Plaintiff's and Class Members' privacy rights by using the Meta Tracking Pixel and Google Analytics to record and communicate online patients' FIDs and IP addresses alongside their confidential medical communications; and

g) Whether Plaintiffs and Class Members are entitled to damages under the ECPA, CIPA, or any other relevant law.

81. **Superiority**: Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Such treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons or entities a method for obtaining redress on claims that could not practicably be pursued individually, substantially outweighs potential difficulties in management of this class action. Plaintiffs know of no special difficulty to be encountered in litigating this action that would preclude its maintenance as a class action.

CLAIMS FOR RELIEF

COUNT I
Violation of the Electronic Communications Privacy Act
18 U.S.C. § 2510, *et seq*.

82. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

83. Plaintiff brings this claim individually and on behalf of the Class.

84. The Electronic Communications Privacy Act ("ECPA") is codified at 18 U.S.C. § 2510, *et seq*.

85. The ECPA prohibits the intentional interception of the contents of any electronic communication. 18 U.S.C. § 2511.

86. The ECPA provides a private right of action to any person whose electronic communications are intercepted. 18 U.S.C. § 2520(a).

87. To state a claim under the ECPA, Plaintiff must plausibly allege that Defendant (1) intentionally (2) intercepted (3) the contents of (4) Plaintiff's electronic communications (5) using a device. *See In re Pharmatrak, Inc.*, 329 F.3d 9, 18 (1st Cir. 2003).

88. Through the use of the Meta Pixel and Google analytics, Defendant intentionally, surreptitiously, and contemporaneously duplicated and forwarded Plaintiff's electronic communications, including sensitive healthcare data, to unauthorized third parties.

89. The transmissions of data between Plaintiff and Class members and VSP qualify as communications under the ECPA. 18 U.S.C. § 2510(12).

90. At all relevant times, VSP engaged Meta and Google to track and intercept Plaintiff's and Class Members' internet communications while accessing VSP's Web Properties. These communications were intercepted without the authorization and consent of Plaintiffs and Class Members.

91. VSP intentionally installed Meta Pixel, Meta App Events, and Google Analytics on its Web Properties and intended to help Meta and Google learn the information and content that users requested and submitted, in real time.

92. Each time Plaintiff and Class Members' information was sent to Meta or Google, these third parties viewed the intercepted information and processed it for their own business purposes—namely, to create targeted advertising based on that information.

93. The Meta Business Tools and similar technologies such as Google Analytics, are "devices" for the purposes of the ECPA. *See Doe v. Meta Platforms, Inc.*, 690 F. Supp. 3d 1064, 1080 (N.D. Cal. 2023) (affirming that the Meta Pixel is a "device" under the ECPA); *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1084 (N.D. Cal. 2015) (affirming that a similar tracking technology which forwarded customer data to a company is a "device" under the ECPA).

94. As alleged above, VSP violated the ECPA by aiding and permitting third parties to receive its users' online communications through its website without their consent.

95. In inducing and communicating private patient information to Meta and Google VSP's intent was tortious, criminal, and in violation of state laws including the CIPA, through conversion, or as a violation of the HIPAA. Further, Meta and Google's purposefully collected private and sensitive patient information with the intent to gain deeper insights into Class members in furtherance of their advertising businesses.

96. Plaintiffs and Class members seek relief under 18 U.S.C. § 2520 including reasonable fees and damages in the amount of whichever is greater, (a) actual damages and any profits made by the violator as a result of the violation or (b) statutory damages of whichever is greater, $100 a day for each violation or $10,000. 18 U.S.C. § 2520.

COUNT II
Violation of the California Invasion of Privacy Act
Cal. Penal Code § 631

97. Plaintiffs incorporate the preceding paragraphs as if fully set forth herein.

98. Plaintiff brings this claim individually and on behalf of the Class.

99. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code § 630, *et seq*.

100. California Penal Code § 631(a), is violated if "by means of any machine, instrument, or contrivance, or in any other manner," a person either:

a) Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system;
b) willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state;
c) uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained; or
d) aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

101. Section 631(a) applies to internet communications and thus applies to Plaintiff and Class Members' sensitive health information which was shared by VSP through the Meta Pixel and Google Analytics. *See Javier v. Assurance IQ, LLC*, No. 21-16351, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) ("Though written in terms of wiretapping, Section 631(a) applies to Internet communications. It makes liable anyone who 'reads, or attempts to read, or to learn the contents' of a communication 'without the consent of all parties to the communication.'" (quoting Cal. Penal Code § 631(a))); *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 608 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of consumers' internet browsing histories).

102. VSP's use of Meta Pixel and Google Analytics is a "machine, instrument, contrivance, or . . . other manner" used to engaged in the prohibited conduct at issue here.

103. At all relevant times, VSP engaged Meta and Google to track and intercept Plaintiff's and Class Members' internet communications while accessing VSP Web Properties. These communications were intercepted without the authorization and consent of Plaintiff and California State Law Class Members.

104. VSP intentionally installed Meta Business Tools and Google Analytics on its Web Properties and intended to help Meta and Google learn the information and content that webpage visitors requested and submitted to www.VSP.com, in real time.

105. Each time Plaintiff's and Class Members' information was sent to Meta or Google, these third parties viewed the intercepted information and processed it for their own business purposes—namely to create targeted advertising based on that information.

106. As alleged above, VSP violated CIPA by aiding and permitting third parties to receive its users' online communications through its website without their consent.

107. As a result, Plaintiff and Class Members seek relief under Cal. Penal Code § 631, including statutory damages of $5,000 per violation under Section 637.2.

COUNT III
Violation of the California Invasion of Privacy Act
Cal. Penal Code § 638.51(a)

108. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

109. Plaintiff brings this claim individually and on behalf of the Class.

110. CIPA § 638.51(a) proscribes any "person" from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

111. A "pen register" is a "device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of the communication." Cal. Penal Code § 638.50(b).

112. The Meta Pixel and Google Analytics are "pen registers" because they are device[s] or process[es]" that "capture[d]" the "routing, addressing, or signaling information" from Plaintiff and Class Members' electronic communications. *Id.*

113. At all relevant times, VSP installed the Meta Pixel and Google Analytics—which are pen registers—onto Plaintiff's and Class Members' browsers, and it used the Meta Pixel and Google Analytics to collect Plaintiff's and Class Members' Private Information.

114. Plaintiff and Class Members did not provide their consent to VSP's installation or use of the Meta Pixel and Google Analytics.

115. VSP did not obtain a court order to install or use the Meta Pixel and Google Analytics.

116. Pursuant to Cal. Penal Code § 637.2, Plaintiff and Class Members have been injured by VSP's violations of CIPA § 638.51(a), and each seek statutory damages of $5,000 for each of VSP's violations of CIPA § 638.51(a).

COUNT IV
Violation of the California Confidentiality of Medical Information Act
Cal. Civ. Code § 56, et seq.

117. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

118. Plaintiff brings this claim individually and on behalf of the Class.

119. The California Confidentiality of Medical Information Act, Cal. Civ. Code § 56, *et seq.* ("CMIA") prohibits health care providers from disclosing medical information relating to their patients without a patient's express authorization. Medical information refers to "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care… regarding a patient's medical history, mental or physical condition, or treatment. 'Individually Identifiable' means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual . . . ." Cal. Civ. Code § 56.05.

120. Defendant is a healthcare provider as defined by Cal. Civ. Code § 56.06.

121. Plaintiff and Class Members are patients of VSP and, as a health care provider, VSP has an ongoing obligation to comply with the CMIA's requirements with respect to Plaintiff's and Class Members' confidential medical information.

122. As set forth above, names, addresses, telephone numbers, email addresses, device identifiers, web URLs, IP addresses, and other characteristics that can uniquely identify Plaintiff

and Class Members are transmitted to Meta and Google in combination with insurance information, medical conditions medical concerns, treatment(s) sought by the patients, and other patient searches and queries. This PHI and PII constitutes confidential information under the CMIA.

123. The Facebook ID is also an identifier that allows identification of a particular individual. Along with patients' confidential Private Information, VSP disclosed patients' Facebook IDs.

124. Pursuant to the CMIA, the information communicated to VSP and disclosed to Meta, Google, and other third parties constitutes medical information because it is patient information derived from a health care provider regarding a patient's medical treatment and physical condition and is received in combination with individually identifying information. Cal. Civ. Code § 56.05(i).

125. As set forth above, Facebook views, processes, and analyzes the confidential medical information it receives via the Facebook Tracking Pixel, Conversions API, SDKs, and other Facebook business tools. Facebook then uses the viewed confidential information to create Audiences for advertising and marketing purpose

126. Similarly, Google also views, processes, and analyzes the confidential medical information it receives via Google Analytics. Google then uses the viewed confidential information for advertising and marketing purposes. Defendant failed to obtain Plaintiff's and Class Members' authorization for the disclosure of medical information.

127. Pursuant to CMIA Section 56.11, a valid authorization for disclosure of medical information must: (1) be "clearly separate from any other language present on the same page and . . . executed by a signature which serves no other purpose than to execute the authorization;" (2) be signed and dated by the patient or their representative; (3) state the name and function of the third party that receives the information; and (4) state a specific date after which the authorization expires. The information set forth on VSP's Web Properties, including the website's Privacy Policy and Notice of Privacy Practices, does not qualify as a valid disclosure or authorization.

128. Defendant violated the CMIA by disclosing patients' medical information to Facebook and/or Google along with the patients' individually identifying information.

129. Plaintiff and Class Members seek nominal damages, compensatory damages, punitive damages, attorneys' fees, and costs of litigation for Defendant's violations of the CMIA.

COUNT V
Violation of the Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, et seq.

130. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

131. Plaintiff brings this claim individually and on behalf of the Class.

132. California's Unfair Competition Law ("UCL") prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

133. VSP engaged in unlawful business practices in connection with its disclosure of Plaintiff's and Class Members' Private Information to unauthorized third parties, including Facebook, in violation of the UCL.

134. VSP's acts, omissions, and conduct, as alleged herein, constitute "business practices" within the meaning of the UCL.

135. VSP violated the "unlawful" prong of the UCL by violating, among other things, Plaintiff's and Class Members' constitutional rights to privacy, state and federal privacy statutes, and state consumer protection statutes.

136. VSP's acts, omissions, and conduct also violate the unfair prong of the UCL because those acts, omissions, and conduct offend public policy (including the federal and state privacy statutes and state consumer protection statutes, such as the ECPA, CIPA, CMIA, and HIPAA) and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiff and Class Members.

137. The harm caused by VSP's conduct outweighs any potential benefits attributable to such conduct, and there were reasonably available alternatives to further VSP's legitimate business interests other than VSP's conduct described herein.

138. Plaintiff and Class Members suffered from a loss of the benefit of their bargain with VSP because they overpaid for insurance services they believed included data security sufficient to maintain their Private Information as confidential.

139. As a result of VSP's violations of the UCL, Plaintiff and Class Members are entitled to injunctive relief. This is particularly true since the dissemination of Plaintiff and Class Members' information is ongoing.

140. As result of VSP's violations of the UCL, Plaintiff and Class Members have suffered injury in fact and lost money or property, including but not limited to payments to VSP for services and/or other valuable consideration—for example, access to their private and personal data.

141. Plaintiff and Class Members would not have used VSP's services, or would have paid less for them, had they known VSP was breaching confidentiality and disclosing their Private Information to social media and tech giants, such as Meta, Microsoft, and Google.

142. The unauthorized access to Plaintiff's and Class Members' Private Information has also diminished the value of that information.

143. In the alternative to those claims seeking remedies at law, Plaintiff and Class Members allege that there is no plain, adequate, and complete remedy that exists at law to address VSP's unlawful and unfair business practices.

144. Further, no private legal remedy exists under HIPAA. Therefore, Plaintiff and Class Members are entitled to equitable relief to restore Plaintiff and Class Members to the position they would have been in had VSP not engaged in unfair competition, including an order enjoining VSP's wrongful conduct, restitution, and disgorgement of all profits paid to VSP as a result of its unlawful and unfair practices.

COUNT VI
Conversion

145. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

146. Plaintiff brings this claim individually and on behalf of the Class.

147. Plaintiff and Class Members have a property interest in their internet browsing data and sensitive health information. They have exclusive access and control over their data, and it can only be created and subsequently shared to the sites they navigate and submit it to through their actions.

148. Defendant's surreptitious interception and dissemination of the Plaintiff's and Class Member's data is a wrongful disposition of their property right, in that it deprives the Plaintiff and Class Members of their ability to control access to that property. Defendant has intentionally used the Meta Pixel and Google Analytics to intercept and transmit the Plaintiff's and Class Members' sensitive health information and browsing data without their consent.

149. Damages caused by conversion are the value of the property at the time of conversion, with the interest from that time. For the Plaintiff and Class Members, this is the fair market value of their data at the time of the conversion, which is readily ascertainable due to the data's value to Meta and Google as part of their revenue model described earlier in the complaint.

150. Plaintiff and Class Members are also entitled to punitive damages. By purposefully and non-consensually sharing users' sensitive health information and browsing data with third parties, Defendant has maliciously disregarded Plaintiff's and Members' property rights.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on behalf of himself and the proposed Class respectfully request that the Court enter an order:

A. Certifying the Class and appointing Plaintiff as the Class representative;

B. Appointing Plaintiff's counsel as class counsel;

C. Finding that Defendant's conduct was unlawful, as alleged herein;

D. Awarding declaratory relief against Defendant;

E. Awarding such injunctive and other equitable relief as the Court deems just and proper;

F. Awarding Plaintiff and Class Members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;

G. Awarding Plaintiff and Class Members pre-judgment and post-judgment interest;

H. Awarding Plaintiff and Class Members reasonable attorneys' fees, costs, and expenses; and

I. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury on all matters so triable.

Dated: June 5, 2025

Respectfully submitted,

By: */s/ Dennis Stewart*

Dennis Stewart, CA Bar No. 99152
GUSTAFSON GLUEK PLLC
600 W. Broadway, Suite 3300
San Diego, CA 92101
Telephone: (619) 595-3299

Daniel C. Hedlund (Pro Hac Vice forthcoming)
Daniel J. Nordin (Pro Hac Vice forthcoming)
Mary M. Nikolai (Pro Hac Vice forthcoming)
Bailey Twyman-Metzger (Pro Hac Vice forthcoming)
GUSTAFSON GLUEK PLLC
Canadian Pacific Plaza
120 South Sixth Street, Suite 2600
Minneapolis, MN 55402
Telephone: (612) 333-8844
dhedlund@gustafsongluek.com
dnordin@gustafsongluek.com
mnikolai@gustafsongluek.com
btwymanmetzger@gustafsongluek.com

Kenneth A. Wexler (Pro Hac Vice forthcoming)
Justin N. Boley (Pro Hac Vice forthcoming)
Zoran Tasić (Pro Hac Vice forthcoming)
Gwyneth F. Lietz (Pro Hac Vice forthcoming)
WEXLER BOLEY & ELGERSMA LLP
311 S. Wacker Drive, Suite 5450
Chicago, IL 60606
Telephone: (312) 346-2222
Facsimile: (312) 346-0022
kaw@wbe-llp.com
jnb@wbe-llp.com
zt@wbe-llp.com
gfl@wbe-llp.com

Brett Cebulash (Pro Hac Vice forthcoming)
Kevin Landau (Pro Hac Vice forthcoming)
Joshua Hall (Pro Hac Vice forthcoming)
TAUS, CEBULASH & LANDAU, LLP
123 William St., Suite 1900A
New York, NY 10038
Telephone: (212) 931-0704
Facsimile: (212) 931-0703
bcebulash@tcllaw.com
klandau@tcllaw.com
jhall@tcllaw.com

Attorneys for Plaintiff and Proposed Class